JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 27 No. 12, pp. 141-149, December 2022
https://doi.org/10.9708/jksci.2022.27.12.141

Design of CCTV Enclosure Record Management System based on Blockchain

Kwan Woo Yu*, Byung Mun Lee*, Un Gu Kang*

*Student, Dept. of Computer Engineering, Gachon University, Seongnam-si, Korea
*Professor, Dept. of Computer Engineering, Gachon University, Seongnam-si, Korea
*Professor, Dept. of Computer Engineering, Gachon University, Seongnam-si, Korea

[Abstract]

In this paper, we propose a design of CCTV enlcosure record management system based on blockchain. Since CCTV video records are transferred to the control center through enclosure, it is very important to manage the enclosure to prevent modulation and damage of the video records. Recently, a smart enclosure monitoring system with real-time remote monitoring and opening and closing state management functions is used to manage CCTV enclosures, but there is a limitation to securing the safety of CCTV video records. The proposed system detect modulated record and recover the record through hash value comparison by distributed stored record in the blockchain. In addition, the integrity verification API is provided to ensure the integrity of enclosure record received by the management server. In order to verify the effectiveness of the system, the integrity verification accuracy and elapsed time were measured through experiments. As a result, the integrity of enclosure record (accuracy: 100%) was confirmed, and it was confirmed that the elapsed time for verification (average: 73 ms) did not affect monitoring.

▸ **Key words**: Blockchain, Integrity Verification System, CCTV Enclosure, Enclosure data management, Monitoring System

[요 약]

본 연구에서는 공공 CCTV 함체 관리를 위한 블록체인 기반 함체기록 관리 시스템을 설계하였다. CCTV 영상 기록은 함체를 거쳐 관제센터까지 전송되기 때문에 영상기록의 변조 및 훼손 방지를 위한 함체 관리가 매우 중요하다. 최근 CCTV 함체 관리를 위해 실시간 원격 모니터링 및 개폐 상태 관리 기능을 갖춘 스마트 함체 모니터링 시스템을 사용하고 있으나 CCTV 영상기록의 안전성 확보에는 한계가 있다. 우리가 제안한 시스템은 함체기록을 블록체인에 분산 저장하여 해시값 비교를 통해 위조를 탐지하고 위조된 함체기록을 복구할 수 있다. 또한 관리서버가 수신하는 함체기록의 무결성을 확인할 수 있도록 무결성 검증 API를 제공하여 함체기록의 무결성을 보장한다. 제안 시스템의 효용성을 검증하기 위해 실험을 통해 무결성 검증 정확도와 소요시간을 측정하였다. 실험 결과 함체기록의 무결성(정확도: 100%)을 확인하였고, 검증 소요시간(평균: 73ms)이 모니터링에 영향을 미치지 않을 것으로 확인하였다.

▸ **주제어**: 블록체인, 무결성 검증 시스템, CCTV함체, 함체기록관리, 모니터링 시스템

• First Author: Kwan Woo Yu, Co-author: Byung Mun Lee, Corresponding Author: Un Gu Kang
*Kwan Woo Yu (dbrhksdn99@gachon.ac.kr), Dept. of Computer Engineering, Gachon University
*Byung Mun Lee (bmlee@gachon.ac.kr), Dept. of Computer Engineering, Gachon University
*Un Gu Kang (ugkang@gachon.ac.kr), Dept. of Computer Engineering, Gachon University
• Received: 2022. 11. 15, Revised: 2022. 12. 01, Accepted: 2022. 12. 05.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

공공 CCTV(Closed Circuit Television)시설물은 CCTV와 함체로 구성되며 화재예방과 방범용으로 설치되어 통합 관제센터에서 운영한다[1]. 설치되는 공공 CCTV는 해마다 증가되고 있으며 2015년 739,232대에서 2021년 1,458,465대로 약 2배가 되었다[2]. 시설물의 증가에 따라 관리에 대한 중요성이 커지고 있기 때문에 개인정보보호위원회에서는 '공공기관 영상정보처리기기 설치운영 가이드라인'을 제정하여 운영하고 있다[3]. 그 가이드라인은 개인정보보호법에 근거를 두고 있어 영상정보 관리에 초점을 맞추고 있다[1,3]. 하지만 영상정보는 CCTV에서 함체를 거쳐 관제센터까지 전송되기 때문에 원활한 영상 확보를 위해선 함체 관리도 중요하다. 따라서 통합 관제센터는 함체의 손상과 장애 예방 그리고 신속한 대응을 위해 스마트 함체 모니터링 시스템을 사용한다[4,5]. 스마트 함체 모니터링 시스템은 함체의 내부 센서 정보와 장치들의 작동정보를 기록한 함체기록을 관리서버에 전송하여 원격으로 운영 상태를 모니터링 하는 시스템이다[6,7].

하지만 스마트 함체는 공원이나 도로 또는 주택가 골목과 같은 실외에 설치되기 때문에 비인가자의 접근에 취약하다. 예를 들어 모니터링 중 장애가 발생하면 작업자는 현장에 출동하여 함체의 잠금장치를 해제하고 내부 장비를 수리하게 된다. 그런데 수리 후 작업자의 부주의로 함체를 열어둔 채 현장을 이탈한다면 비인가자가 승인 없이 함체 내부로 접근 할 수 있다. 설령 함체기록을 관리서버로 전송한다 하더라도, 함체기록만으로는 현장상태를 확인할 방법이 없다. 또한 함체에서 관리서버로 보내는 함체기록이 암호화되지 않은 상태라면 비인가자는 전송되는 함체기록을 위조할 수 있다는 취약점도 생긴다. 따라서 저장된 함체기록의 무결성 유지가 필요하다.

본 연구에서는 이러한 문제점을 해결하기 위해 함체기록 관리에 블록체인을 도입하고자한다. 블록체인은 블록단위로 데이터를 분산저장하여 데이터 위조 시 복구가 가능하고, 블록 해시를 통해 데이터 무결성을 보장할 수 있다. 제안하는 블록체인 기반 함체기록 관리 시스템은 함체에서 동작하며 블록체인 네트워크를 이루어 함체기록을 분산저장하고 현재 블록 해시와 이전 블록 해시를 비교하여 저장된 기록의 위조 유무를 확인할 수 있다. 그리고 블록체인은 무결성 검증 API를 제공하여 관리서버에서 수신한 함체기록의 무결성 침해를 탐지할 수 있다.

2장은 관련연구로 블록체인 분산저장 기술 및 스마트 함체 모니터링 시스템에 대해 살펴보고, 3장에서는 블록체인 기반 함체기록 관리 시스템을 제안한다. 4장에서 실험 및 평가를 통해 제안한 시스템의 효용성을 평가하고, 마지막 5장에서는 실험 및 평가를 토대로 결론을 기술한다.

II. Related works

1. Smart Enclosure Monitoring System

스마트 함체 모니터링 시스템은 스마트 함체와 스마트 함체의 작동 상태를 모니터링하는 관리서버, 그 서버와 연결되어 있는 함체에 대해 제어명령을 송신하는 통합 관리 소프트웨어를 포함하는 함체 관리 시스템으로 Fig. 1과 같이 동작한다[8]. 스마트 함체는 Fig. 2와 같이 내부 센서 데이터의 측정값과 기기 동작 상태를 측정한 함체기록을 내부 로그파일에 저장하고 주기적으로 로그파일에 저장한 함체기록을 읽어와 서버로 송신한다. 서버는 수신한 정보를 통해 관리자에게 모니터링 기능을 제공하고 관리자의 조작에 따라 함체의 냉각 장치 작동, 잠금장치 해제 등의 명령을 함체에게 송신한다[8,9]. Fig. 2의 상황에 따른 분석과 대처는 관리서버로부터 명령을 받아 수행한다. 그러므로 함체가 송신하는 함체기록은 시스템의 정상 작동을 위해 중요한 역할을 한다.

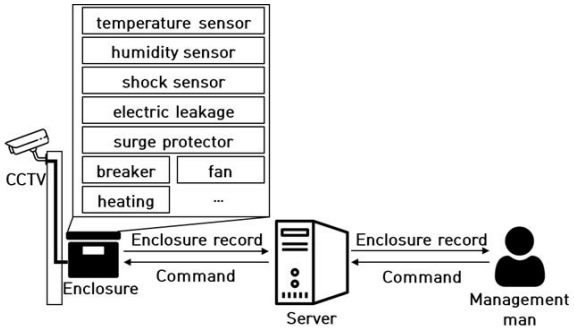


Fig. 1. Control process of smart enclosure monitoring system.

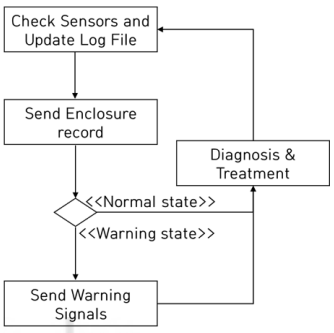


Fig. 2. Operation process of smart enclosure.

이때 함체가 송신하는 함체기록은 Table 1과 같으며 내부에 있는 센서의 기록과 장치 동작 상태로 구성되어 있다. 센서기록은 문 열림 감지 센서정보, 내부 온도, 내부 습도, 충격 발생정보로 구성되어 있고 장치 동작 상태는 잠금장치 잠금 여부, 누전 차단기동작 상태, 서지 보호기 동작 상태, 온도조절 장치 동작 상태로 구성되어 있다[6,7]. 이 함체기록을 통해 Fig. 1의 관리자는 직접 함체를 방문점검 하지 않아도 함체와 장비의 상태를 알 수 있고 적절한 동작 명령을 판단하여 내릴 수 있다.

Table 1. Sensors record of smart enclosure.

Name	Description
Door	Door open state
Lock	Lock operation state
Elb	Electric Leakage Breaker operation state
Surge	Surge protector state
Heating	Heating operation state
Fan	Fan operation state
Temperature	Internal temperature
Humid	Internal humidity
Outlet	Outlet operation state
Power	Watt by outlet port
Shocklevel	Degree of shock
Shocktime	Timestamp of shock

스마트 함체 내부에 있는 로그파일이 위조되는 경우 관리서버가 수신하는 함체기록이 위조될 수 있다. 스마트 함체는 주로 보행로 옆이나 차로 옆에 설치되고 수리의 용이성을 위해 손이 닿기 쉽도록 설치 높이가 낮기 때문에 비인가자의 내부 접근을 방지하기 위해 잠금장치를 사용한다. 하지만 내부 장비 수리를 위해 현장 작업자가 잠금장치를 해제한 후 부주의로 인해 잠금장치를 잠그지 않고 자리를 이탈하는 경우 비인가자의 내부 접근이 가능해진다. 이때 비인가자는 내부 장치 접근을 통해 로그파일을 위조하여 함체기록을 위조할 수 있다. 이와 같이 함체기록이 위조되는 경우 관리서버가 잘못된 명령을 내려 장비의 고장을 일으키거나 장비의 수명이 줄어들 수 있다.

2. Blockchain

블록체인은 정보를 중앙 서버가 아닌 각각의 노드가 관리하는 분산저장 시스템의 일종으로 블록이라는 구조로 데이터를 저장하고 해시 알고리즘을 이용하여 무결성을 보장한다[10]. 해시 알고리즘은 데이터 원문을 추정하기 어려울 정도로 가공하여 원문을 보호하고 쇄도효과(Avalanche effect)로 해시값을 비교하여 무결성 침해를 판단할 수 있다[11]. 각 노드는 블록체인의 무결성이 침해된 경우 다른 노드에 분산저장된 블록체인을 통해 복구한다[12]. 블록체인은 Fig. 3과 같은 구조로 저장된다. 블록체인 난이도에 맞는 블록 해시(Block hash)와 논스(Nonce)값을 생성하고 이전 블록 해시(Previous block hash)를 가져 다음 블록임을 논리적으로 나타낸다[13]. 이 블록 해시와 이전 블록 해시를 통해 모든 블록 해시가 상관관계에 있도록 하여 블록체인의 무결성을 증명한다.

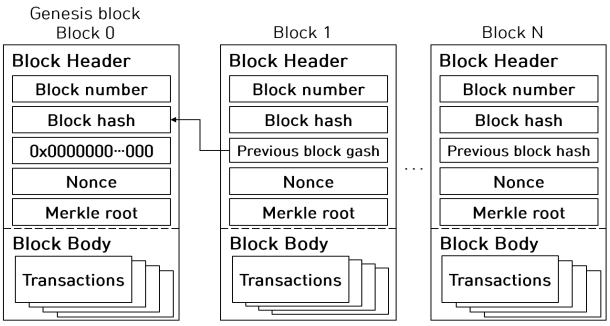


Fig. 3. Blockchain data structure.

블록체인은 블록체인 네트워크에 참여하는 노드의 권한에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 구분할 수 있다[14,15]. Table 2는 퍼블릭 블록체인과 프라이빗 블록체인의 특성을 나타낸다. 퍼블릭 블록체인은 모든 노드가 블록을 검증하고 생성할 수 있는 블록체인으로 별도의 허가 없이 모든 블록에 접근이 가능하다[16]. 하지만 모든 노드의 검증을 거치기 때문에 트랜잭션 처리 속도가 느리고 모든 노드가 블록을 생성할 수 있어 악의적인 노드의 블록 생성이 가능하다. 프라이빗 블록체인은 허가된 노드만 참여하여 블록을 검증하고 생성할 수 있으며 블록에 접근이 가능하다[17]. 그러므로 허가된 노드의 검증만 거치기 때문에 트랜잭션 처리 속도가 빠르고 악의적인 노드의 블록 생성이 불가능하다[18].

Table 2. Properties of public blockchain and private blockchain.

Property	Public blockchain	Private blockchain
Data access permission	Anyone	Permissioned member
Anyone can join	Yes	Permissioned node
Generate block permission	Any node	Permissioned node
Average transactions per second	5 ~ 40 TPS	1000 TPS
Consensus protocol	Proof of Work, Proof of Stake	Varies

함체기록을 관리하기 위한 블록체인은 위조된 함체기록이 블록체인에 기록되지 않도록 해야 한다. 그러므로 본 연구에서는 함체기록 관리 블록체인을 프라이빗 블록체인으로 관리한다.

III. Enclosure record management based on blockchain

1. Enclosure record management system based on blockchain

본 연구에서는 스마트 함체의 함체기록 관리에 블록체인을 적용한 블록체인 기반 함체기록 관리 시스템을 제안한다. 제안 시스템은 기존 스마트 함체 모니터링 시스템의 문제점을 해결하기 위해 함체에 저장하는 함체기록의 신뢰성을 확보하고 무결성을 유지해야 한다. 또한 관리서버가 수신하는 함체기록을 검사하여 무결성이 침해되었는지 확인할 수 있어야 한다.

Fig. 4는 블록체인 기반 함체기록 관리 시스템의 구성도이다. 시스템은 스마트 함체, 블록체인 그리고 관리서버로 구성한다. 함체기록을 로그파일 대신 블록체인에 분산저장하므로 조작에 대한 취약성을 줄인다(①). 그리고 블록체인에 저장한 신뢰할 수 있는 함체기록을 읽어 관리서버로 전송한다(②, ③). 관리서버가 수신한 함체기록을 검사하여 방문 점검 없이 위조여부를 확인할 수 있도록 블록체인에 기반한 무결성 검증 API를 구성한다(④, ⑤, ⑥, ⑦). 같은 블록체인 네트워크에 참여하는 모든 스마트 함체는 같은 블록체인을 유지하여 다른 함체의 함체기록을 검증하더라도 동일한 결과를 받을 수 있도록 하여 장애가 발생 시 무결성 검증을 받을 수 있도록 한다. 예를 들어 Fig. 4의 함체 2(Enclosure 2)의 함체기록을 함체 4(Enclosure 4)가 제공하는 무결성 검증 API를 통해 검증이 가능하다.

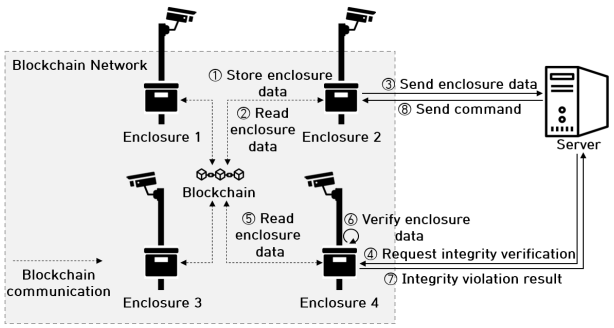


Fig. 4. Configuration of blockchain-based enclosure record management system.

제안한 시스템에서는 함체기록을 블록체인에 저장하고 그 함체기록을 읽어와 전송하기 때문에 함체기록의 위변조를 예방 및 복구할 수 있을 뿐 아니라 무결성도 유지될 수 있다. 또한 실시간 모니터링을 위한 가용성도 만족되어야 하므로 다음 절에서 함체기록 저장형식과 과정을 정의한다.

2. Process of store and maintain of enclosure record

함체기록 저장 과정은 스마트 함체에서 생성되는 데이터와 기록을 블록체인에 저장하는 과정을 말한다. 이 과정에서는 기록이 정상 함체에서 발생한 함체기록인지 악의적인 공격자가 위조한 함체기록인지를 먼저 구분해야 한다. 그러므로 Fig. 5의 과정을 거쳐 블록체인에 저장하고 Table 3과 같은 구조의 블록을 사용한다. Fig. 5는 함체 기록을 블록체인에 저장하는 과정으로, 함체는 내부 온습도, 충격감지센서, 문 열림 감지센서와 같은 센서정보를 읽어와 함체기록을 생성하는데 개인키(private)를 사용하여 암호화한다. 그리고 블록체인 난이도에 맞는 블록 해시를 생성한다. 이후 생성한 블록을 다른 함체에게 배포하여 이 블록을 수신한 함체들이 이전 블록 해시와 비교하고 블록해시가 정상인지 확인할 수 있도록 한다. 그리고 암호화된 함체기록은 공개키(public)로 복호화하여 신뢰할 수 있는 함체가 생성한 블록인지를 확인할 수 있게 한다. 블록해시를 통한 검증결과와 복호화 결과가 모두 정상이면 정상 함체에서 발생한 함체기록으로 구분하고 블록체인에 저장한다.

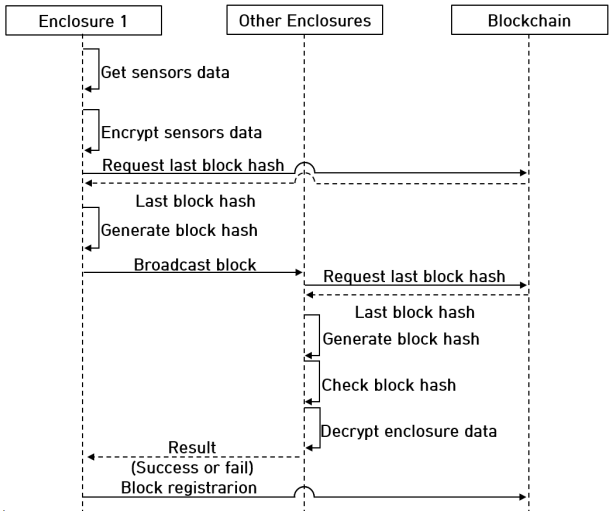


Fig. 5. Process of storing block on blockchain.

Table 3. Structure of block.

Component	Name
Header	Block Hash
	Previous Block Hash
	Nonce
	Timestamp
	Enclosure ID
Body	Encrypted sensors data

함체기록은 Fig. 5와 같은 과정을 통해 안전하게 저장되며, 저장된 블록은 해시 알고리즘으로 무결성을 유지하는데, 블록을 구성하는 데이터 중 하나라도 변경 된다면 함체기록을 읽을 수 없어 블록전체의 무결성이 유지가 필요하다. 따라서 Fig. 6와 같이 블록 해시를 생성하여 블록을 구성하는 데이터 중 하나라도 변경 된다면 알 수 있도록 한다. 이를 위해서 블록을 생성할때 이전 블록 해시(previous block hash), 논스(nonce)와 함체기록(enclosure record)을 입력받은 후, 함체기록을 암호화하고 함체기록 시간정보(timestamp), 함체 식별자(Enclosure ID), 이전 블록 해시(previous block hash), 논스(nonce), 암호화된 함체기록(encrypted enclosure data)을 기반으로 블록 해시를 생성한다.

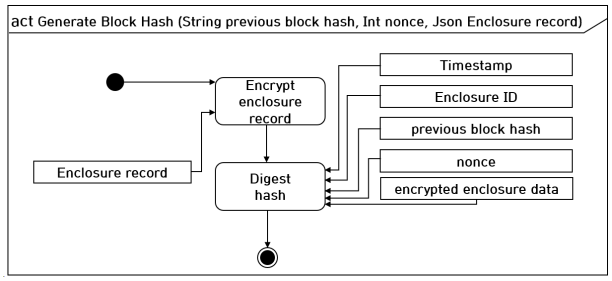


Fig. 6. Process of generate block hash.

이와 같은 과정으로 블록체인에 저장된 블록의 무결성이 유지될 수 있다. 관리서버에서는 함체에서 받은 기록을 사용하기 전에 검증하여야 하는데 다음 절에서 함체기록의 무결성 검증을 정의한다.

3. Verification of enclosure record integrity

함체기록 무결성 검증은 관리서버가 수신한 함체기록을 블록체인에 저장된 함체기록과 비교하여 무결성이 훼손되었는지 검증 한다. 이 검증은 관리서버의 실시간 모니터링 시스템의 가용성을 만족해야 한다. 검증 과정은 Fig. 7에서 보는 바와 같이 서버가 함체에게 수신한 함체기록의 검증을 요청하고, 함체는 이를 수신하여 해당 함체기록이 저장된 블록을 블록체인에서 찾아 암호화된 함체기록을 복호화 한 후 센서기록을 비교하여 무결성이 침해 되었는지를 확인한 후, 관리서버에게 결과를 반환한다. 이러한 검증 과정을 통해 서버는 무결성 검증 결과를 수신하여 기록의 위조여부를 알아낼 수 있다.

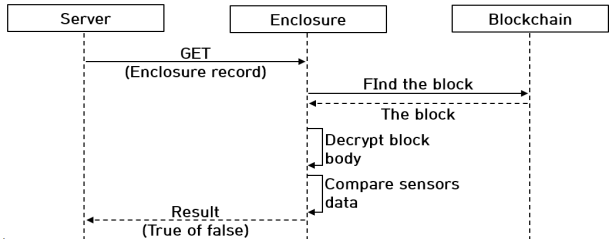


Fig. 7. Process of enclosure record verification.

검증 과정에서 기존 함체기록을 사용하는 경우 블록에 저장하는 함체기록이 암호화 되어 저장하기 때문에 검증 요청이 발생할 때 마다 해당하는 블록을 찾기 위해 모든 암호화된 함체기록을 복호화 해야 한다. 이는 성능을 저하시키고 실시간 모니터링 시스템의 가용성을 해친다. 따라서 Fig. 8과 같은 구조의 함체기록을 사용한다. 함체기록은 함체 식별자(Enclosure ID)와 함체기록 저장 시각(Timestamp), 센서기록(Sensors data)으로 구성 되며 센서기록은 2.1절의 스마트 함체의 센서기록이다. 블록은 3.2절의 블록 구조와 같이 헤더(Header)에 암호화 되지 않은 함체 식별자(Enclosure ID)와 함체기록 저장 시간(Timestamp)이 저장되기 때문에 함체 식별자와 함체기록 저장 시간으로 블록을 특정할 수 있어 모든 암호화된 함체기록의 복호화 없이 찾을 수 있다.

Component	Name
Enclosure record	Enclosure ID
	Timestamp
	Sensors data

Name	Description
Door	Door open state
Lock	Lock operation state
Elb	Electric Leakage Breaker operation state
Surge	Surge protector state
Heating	Heating operation state
Fan	Fan operation state
Temperature	Internal temperature
Humid	Internal humidity
Outlet	Outlet operation state
Power	Watt by outlet port
Shocklevel	Degree of shock
Shocktime	Timestamp of shock

Fig. 8. Structure of enclosure record.

블록체인 기반 함체기록 관리 시스템은 이와 같은 무결성 검증을 통해 저장된 함체기록의 무결성을 유지한다.

이어서 4장에서는 실험을 통해 제안 시스템의 성능을 평가한다.

IV. Experimental Evaluation

1. Experimental conditions

본 실험에서는 블록체인 기반 함체기록 관리 시스템에서 제공하는 무결성 검증 API가 정확히 동작하는지 정확도를 측정하여 효용성을 평가하고 소요시간을 측정하여 가용성을 평가한다. 실험 환경은 서울시 CCTV통합 관제센터별 함체관리 자료를 최대한 고려하여 실제 상황과 유사하게 실험 한다[2,19]. 장애 발생시간 4시간 이내에 1만개부터 15만개의 함체기록이 저장된 환경에서 무결성 검증 API가 동작되는지 확인하는 실험을 하였다[20].

실험을 위한 블록체인 노드는 Table 4의 사양을 가진 Raspberry Pi를 사용하였으며 라즈비안 커널버전 5.10을 설치하여 Node.js 16.13.1 플랫폼을 사용하였다. 서버는 Table 5의 사양으로 Windows 10 21H2버전을 설치하여 Node.js 16.13.1 플랫폼을 사용하였다. 실제 실험 환경은 Fig. 9와 같으며 10대의 블록체인 노드(a)에서 시스템을 가동하였고 서버(c)에서 무결성 검증 요청을 실시한 뒤 서버 모니터(b)를 통해 결과 로그를 확인하였다.

Table 4. Specification of raspberry pi.

Type	Specifications
Model	Raspberry Pi 4 Model B 2GB
CPU	Broadcom BCM2711 @ 1.5GHz
RAM	2GB LPDDR4-3200 SDRAM
OS	Raspberry Pi OS kernel v 5.10

Table 5. Specification of server.

Type	Specifications
CPU	AMD Ryzen 5 2400G @ 3.6GHz
GPU	AMD Radeon RX Vega 11
RAM	16GB DDR4-3200 SO-DIMM
OS	Windows 10 version 21H2

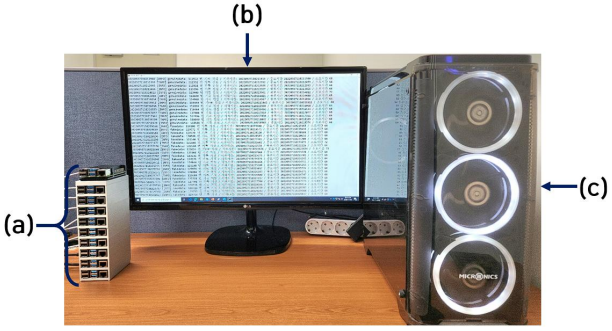


Fig. 9. Experiment environment for enclosure record verification. (a)set of 10 blockchain nodes, (b) log file on server, (c) server

실험은 Fig. 9의 (a)인 각 블록체인 노드에서 각각 시스템을 실행하여 기록을 분산 저장하였다. 이후 Fig. 9의 (c)에서 100회의 무결성 검증을 요청하고 평균 소요시간과 정확도를 측정하였다. 측정한 소요시간은 Fig. 10와 같이 서버에서 노드로 검증 요청이 전송되는 시간(T_1), 노드가 블록체인에서 블록을 찾는 시간(T_2), 센서 데이터를 비교하여 무결성 검증을 하는 시간(T_3), 마지막으로 검증 결과가 서버로 도착하는 시간(T_4)을 포함한 시간으로 식(1)과 같이 정의한다.

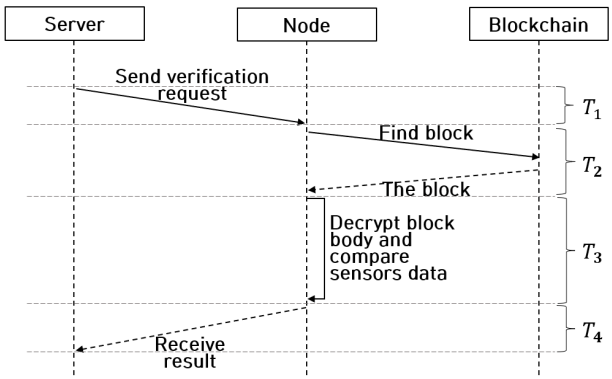


Fig. 10. Process of integrity verification.

$$ElapsedTime = \sum_{i=1}^{4} T_i \qquad (1)$$

실험에 사용하는 함체기록은 위조된 함체기록과 무결한 함체기록 모두 검증이 잘 이루어지는지 확인할 수 있도록 50개의 위조된 함체기록과 50개의 무결한 함체기록으로 구성하였다.

2. Elapsed time and accuracy for verification

실험은 100회의 검증을 통해 각각의 검증결과와 소요시간을 측정하여 평균 소요시간과 정확도를 계산하였다. 실험 결과 함체기록의 개수별 평균 소요 시간은 Fig. 11과 같으며 1만개의 함체기록이 저장되었을 때 가장 낮은 평균 소요 시간인 58ms가 측정되었고 15만개의 함체기록이 저장되었을 때 가장 높은 평균 소요시간인 73ms가 측정되었다. 함체기록이 증가할수록 완만한 증가세를 보였고 관리서버의 모니터링을 위한 가용성을 해치지 않았음을 확인하였다.

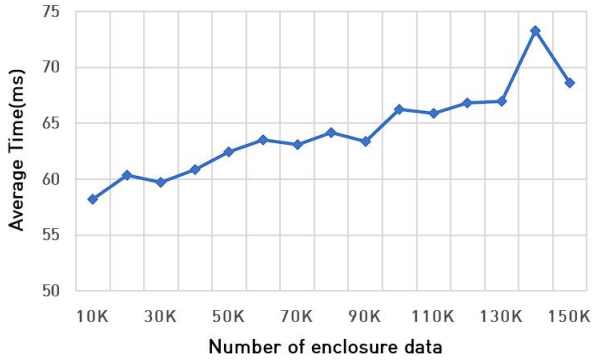


Fig. 11. Average elapsed time of verification by number of blocks.

Table 6는 혼돈 행렬(confusion matrix)에 기반하여 함체기록 개수별 검증 결과를 나타낸 것으로, 혼돈 행렬은 ①무결한 함체기록을 무결하다고 정확하게 검증한 빈도수(TP: True Positives), ②위조된 함체기록을 위조 되었다고 정확하게 검증한 빈도수(TN: True Negatives), ③무결한 함체기록을 위조되었다고 잘못 검증한 빈도수(FP: False Positives), ④위조된 함체기록을 무결하다고 잘못 검증한 빈도수(FN: False Negatives)로 이루져 있으며, 이 4가지 정보를 바탕으로 무결성 검증 API가 정확히 동작하는지 정확도를 측정하였다. 식(2)는 정확도를 계산하는 수식으로, 무결한 것은 무결로, 위조된 것은 위조로 정확히 검증해 내는 것을 의미하며, 무결성 검증 API가 얼마나 정확히 동작하는지 평가는 척도이다. 검증 결과, 모든 블록에서 무결한 함체기록 50개와 위조된 함체기록 50개에 대해 모두 올바른 판단을 하였고 무결성 검증 정확도 100%를 기록하였다.

Table 6. Verification results and accuracy

Number of enclosure data	TP	FP	FN	TN	Accuracy(%)
10,000	50	0	0	50	100
20,000	50	0	0	50	100
30,000	50	0	0	50	100
40,000	50	0	0	50	100
50,000	50	0	0	50	100
60,000	50	0	0	50	100
70,000	50	0	0	50	100
80,000	50	0	0	50	100
90,000	50	0	0	50	100
100,000	50	0	0	50	100
110,000	50	0	0	50	100
120,000	50	0	0	50	100
130,000	50	0	0	50	100
140,000	50	0	0	50	100
150,000	50	0	0	50	100

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (2)$$

본 연구에서 제안한 블록체인기반 함체기록 관리시스템은 최대 평균 소요시간 73ms 와 정확도 100%의 무결성 검증 API를 제공하여 효용성과 가용성을 만족함을 확인할 수 있었다.

3. Stored data management

Table 7은 기존 스마트 함체 모니터링 시스템과 본 연구에서 제안한 블록체인 기반 함체기록 관리 시스템의 함체기록 관리를 비교한 결과이다. 데이터 복구에 관한 항목은 기존 시스템이 분산저장 없이 함체 내부에 저장되기 때문에 블록체인으로 데이터를 분산저장하는 제안한 시스템에 비해 데이터 무결성 훼손에 취약하고 복구에 어려움이 있다. 데이터 위조 공격과 위조된 데이터 확인에 관한 항목은 기존 시스템이 공격에 의한 데이터 위조가 발생하여도 이를 확인할 수 없어 블록해시로 위조를 탐지할 수 있는 제안한 시스템에 비해 공격에 취약하다. 또한 제안한 시스템은 관리서버에 함체기록에 대한 무결성 검증 API를 제공하여 관리서버가 수신하는 데이터 위조에 성공하여도 관리서버가 알 수 있도록 한다.

Table 7. Comparison of stored data smart enclosure monitoring system and enclosure record management system based on blockchain

Comparison factor	Smart enclosure monitoring system	Enclosure record management system based on blockchain
Data recovery	Weak (Internal storage)	Strong (Distributed storage)
Security against attacks	Weak (Internal storage)	Strong (Distributed storage)
Tampered data check	No	Yes (Block hash)
Integrity verification	No	Yes (Integrity verification API)

V. Conclusions

본 연구에서는 기존 스마트 함체 모니터링 시스템의 함체기록 문제점을 해결하기 위해 블록체인 기반 함체기록 관리 시스템을 제안하였다. 제안한 시스템은 함체기록을

블록체인에 분산 저장하여 해시값 비교를 통해 위조를 탐지하고 위조된 함체기록을 복구할 수 있다. 또한 관리서버가 수신하는 함체기록의 무결성을 확인할 수 있도록 무결성 검증 API를 제공하여 현장 점검 없이 무결성이 침해되었는지 알 수 있도록 하였다. 실제 환경과 유사한 실험 환경에서 실험을 통해 제안 시스템의 가용성과 효용성을 확인하였다. 제안한 시스템을 스마트 함체 모니터링 시스템에 적용한다면 비인가자의 공격이 발생하여도 원본 함체기록을 지킬 수 있으며 현장 점검 없이 공격 사실을 알 수 있어 효율적인 모니터링이 가능할 것으로 판단된다.

향후 연구에서는 실제 시스템이 동작하는 하드웨어를 제작하고 스마트 함체에 장착하여 성능 평가를 진행하고 데이터 저장 시 병목 현상을 개선하고자 한다.

ACKNOWLEDGEMENT

This work was supported by the Technology development Program(Grants No. S3229617) funded by the Ministry of SMEs and Startups(MSS, Korea).

REFERENCES

[1] Kim Ji-Sun, "Operational Improvement of Integrated Control Center through Analysis of CCTV Research", korean Journal of Public Safety and Criminal Justice, vol. 23, no. 2, pp 65-96, June, 2014

[2] Statistics Korea, “Installation and operation of CCTV in public institutions”, http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=2855

[3] Personal Information Protection Commission, “Guidelines for Installation and Operation of CCTV”, https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?mCode=D010030000

[4] CHANG IL SIK, Park JongCheol, “Integrated CCTV Control Center: Operational Performance and Improvement Plan – Based on Gumi-si –”, Police science journal, vol 13, no. 1, 211-246, January, 2018, DOI: 10.16961/polips.2018.13.1.211

[5] Park Mun Su, Lee Hiyong, Byounghee Kim, “A Study on the Demonstration of Data-Based Performance in Smart City”, The Journal of Information Technology and Architecture, vol 17, no.1, 51-61, March, 2020, DOI: 10.22865/jita.2020.17.1.51

[6] U-sys, “Smart remote monitoring control system”, https://doi.org/10.8080/1020200071339

[7] U-sys, “SYSTEM FOR MONITORING ASSEMBLING-DISMANTLING TYPE POWER SUPPLY APPARATUS”, https://doi.org/10.8080/1020170116035

[8] Yeong-Yil Yang, Young-Sik Park, Hyeon-Jong Lee, Young-Ho Choi, Jong-Chul Lee, “Multi-Channel Housing Monitoring System”. Information and Control Symposium, 93-96, Jukjeon, Korea, April, 2016

[9] Kim Hee-Chul, “Internal communication as CCTV Automatic Climate Control System Development”, The Journal of the Korea Institute of Electronic Communication Sciences, vol.10, no. 4, 433-439, April, 2015, DOI: 10.13067/JKIECS.2015.10.4.433

[10] DaeYoub Kim, “A Study on a Smart Home Access Control using Lightweight Proof of Work” , Journal of IKEEE, vol. 24, no. 4, 11-21, December, 2020, DOI: 10.7471/ikeee.2020.24.4.931

[11] Ahn, Ka Kyung. “A Convergent Study of Block Chain and Mathematical Algorithms”, The Korean Society of Science & Art , vol. 37, no. 1, 137-147, January, 2019, DOI: 10.17548/ksaf.2019.01.30.137

[12] Daehwa Rayer Lee, Hyoungshick Kim, “Blockchain Research Trend Analysis: Focusing on Consensus Algorithm”. REVIEW OF KIISC, vol. 28, no. 3, 5-10, June, 2018

[13] Hong Ki Hyeon, Lee Byung Mun, “An Access Code Key for Verification Service Model on the Blockchain in a Door Security”, Journal of Korea Multimedia Society, vol. 25, no. 10, 1416-1432, October, 2022, DOI: 10.9717/KMMS.2022.25.10.1416

[14] Ji-Sun Park, Sang Uk Shin, “Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection”, Journal of Internet Computing and Services, vol. 24, no. 6, 105-117, December, 2019, DOI: 10.7472/JKSII.2019.20.6.105.

[15] Han Hyegyeong, Hwang Heejoung, “Hyperledger Fabric and Asymmetric Key Encryption for Health Information Management Server”, Journal of Korea Multimedia Society, vol. 25, no. 7, 922-931, July, 2022, DOI: 10.9717/KMMS.2022.25.7.922

[16] Lee Sae Bom, Song Jaemin, “Blockchain Technology and Application”, Journal of the Korea Society of Computer and Information, vol. 26, no. 2, 89-97, February, 2021, DOI: 10.9708/JKSCI.2021.26.02.089

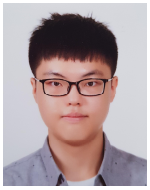
[17] Jong-Woo Leew, Hyeong-Jin Kim, Jae-Min Lee, Tae-Soo Jun, Dong-Seong Kim, “Blockchain-Based Data Sharing Scheme to Enhance Reliability and Security for Naval Combat Systems”, vol. 47, no. 06, 809-817, June, 2022, DOI: 10.7840/kics.2022.47.6.809

[18] Minho Kim, Sujin Kim, Hoon Choi, “Algorithm for Detecting Double-Spending in Blockchain”, vol. 45, no. 8, 858-855, August, 2018, DOI: 10.5626/JOK.2018.45.8.848

[19] Ministry of Public Administration and Security, “Local data of cctv”, https://www.localdata.go.kr/lif/lifeCtacDataView.do

[20] Goesan-gun, “Work instruction of CCTV integrated control system maintenance service”, https://www.goesan.go.kr/www/selectBbsNttView.do?key=137&bbsNo=214&nttNo=55291

Authors



Kwan Woo Yu is currently third year B.S. student in Department of Dept. of Computer Engineering at Gachon University in Korea. His research interests include IoT Smart Service and blockchain.

Byung Mun Lee received a B.S. degree in 1988 from Dongguk University, Seoul, Korea and a M.S. degree from Sogang University and a Ph.D. degree from University of Incheon Korea, in 1990 and 2007.

He had worked for LG Electronics for 7 years. He is currently a professor in the department of Computer Engineering, Gachon University, South Korea. He had been at California State University Sacramento, USA from 2013 to 2014 as a visiting scholar. His research interests are IoT for healthcare, AIoT Smart Service, network protocols, blockchain, smart services, etc.

Un Gu Kang received Ph.D. degree in Computation Engineering from Inha University in 2001. He is currently a Professor in Department of Computer Engineering at Gachon University.

His primary research interests include Mobile Software, Healthcare Information, U-healthcare.